CLAIMS

1. A method of limiting unauthorized network requests, comprising the steps of:

identifying entities legitimately entitled to service;

establishing said identified entities as trusted entities;

processing requests from said trusted entities according to a first policy; and

processing remaining requests according to at least a second policy.

2. The method of Claim 1, wherein an entity comprises a user ID/client pair.

3. The method of Claim 2, wherein said client comprises any of:

an instance of a client software application; and

a machine running a client software application.

4. The method of Claim 2, wherein entities legitimately entitled to service comprise entities previously able to successfully authenticate to a network service.

5. The method of Claim 4, wherein said network service comprises a server.

6. The method of Claim 4, wherein establishing said identified entities as trusted entities comprises the step of:

issuing a trust token for each entity successfully authenticating to said network service.

7. The method of Claim 6, wherein said trust token comprises a data object.

8. Method of claim 7, said data object including:

said user ID or a derivative thereof.

9. The method of Claim 8, wherein said derivative comprises a cryptographic hash of the user ID.

10. The method of Claim 8, wherein said data object further includes any of:

a time stamp of first authentication to said network service by said entity; and

a time stamp of a most recent authentication to said network service by said entity.

11. The method of Claim 8, said data object including a client identifier.

12. The method of Claim 11, said client identifier comprising any of:

a client identifier assigned by said network service; and

a client identifier provided by the client.

13. The method of Claim 7, further comprising a step of encrypting said trust token.

14. The method of Claim 13, further comprising the step of:

transmitting said trust token from said network service to said client upon successful authentication to said network service by said entity.

15. The method of Claim 14, wherein said step of transmitting said trust token occurs via a secure channel.

16. The method of Claim 15, wherein said secure channel comprises a network connection secured via the SSL (secure sockets layer) protocol.

17. The method of Claim 7, further comprising the step of:

storing said issued trust token on said client.

18. The method of Claim 17, further comprising the step of:

transmitting said stored issued trust token along with said user ID, authentication credentials, and client identifier from said client to said network service.

19. The method of Claim 18, wherein said step of transmitting said stored, issued trust token occurs via a secured channel.

20. The method of Claim 19, wherein said secured channel comprises a network connection secured via the SSL (secure sockets layer) protocol.

21. The method of Claim 12, further comprising a step of storing said issued trust token in a server side database, indexed according to a combination of user ID and client identifier.

22. The method of Claim 21, further comprising the step of:

transmitting said client identifier assigned by said network service from said network service to said client upon successful authentication to said network service by said entity.

23. The method of Claim 22, wherein said step of transmitting said client identifier assigned by said network service occurs via a secure channel.

24. The method of Claim 22, said secure channel comprising a network connection secured via the SSL (secure sockets layer) protocol.

25. The method of Claim 21, further comprising the steps of:

transmitting said user ID and client identifier to said server; and

retrieving said stored trust token from said database.

26. The method of Claim 21, wherein said server side database serves a plurality of services.

27. The method of Claim 2, wherein processing requests from said trusted entities according to a first policy comprises the steps of:

validating said trust token; and

processing request without adding incremental response latency.

28. The method of Claim 27, wherein said step of validating said trust token comprises the step of:

verifying that the user ID and a client identifier in the trust token match those presented by the client on the request.

29. The method of Claim 28, wherein said step of validating said trust token further comprises any of the steps of:

verifying that a time stamp of a first authentication by the entity recorded in the trust token is no earlier than a configurable earliest acceptable first-authentication time stamp; and

verifying that a time stamp of a last authentication by the entity recorded in the trust token is no earlier than a configurable earliest acceptable last-authentication time stamp.

30. The method of Claim 2, wherein processing remaining requests according to at least a second policy comprises adding a configurable amount of incremental response latency when processing untrusted logins.

31. The method of Claim 30, wherein untrusted logins include successful and unsuccessful logins from entities not bearing a trust token.

32. The method of Claim 31, wherein response latency is added to a configurable percentage of successful untrusted logins.

33. The method of Claim 2, wherein processing remaining requests according to at least a second policy comprises adding a configurable amount of incremental response latency when processing requests from untrusted IP addresses that have exceeded a configurable login rate.

34. The method of Claim 2, wherein processing remaining requests according to at least a second policy comprises requiring an untrusted entity to complete a Turing test.

35. The method of Claim 1, wherein said policies are applied by a server.

36. The method of Claim 35, wherein said server applies rate policies for a plurality of network devices.

37. The method of Claim 6, further comprising the step of:

updating said trust token after a login by a trusted entity.

38. A computer program product comprising computer readable code means embodied on a tangible medium, said computer readable code means comprising code for performing a method of limiting unauthorized network requests, said method comprising the steps of:

identifying entities legitimately entitled to service;

establishing said identified entities as trusted entities;

processing requests from said trusted entities according to a first policy; and

processing remaining requests according to at least a second policy.

39. The method of Claim 38, wherein an entity comprises a user ID/client pair.

40. The method of Claim 39, wherein said client comprises any of:

an instance of a client software application; and

a machine running a client software application.

41. The method of Claim 40, wherein entities legitimately entitled to service comprise entities able to successfully authenticate to a network service.

42. The method of Claim 41, wherein said network service comprises a server.

43. The method of Claim 41, wherein establishing said identified entities as trusted entities comprises the step of:

issuing a trust token for each entity successfully authenticating to said network service.

44. The method of Claim 43, wherein said trust token comprises a data object.

45. The method of Claim 44, said data object including:

said user ID or a derivative thereof.

46. The method of Claim 45, wherein said derivative comprises a cryptographic hash of the user ID.

47. The method of Claim 45, wherein said data object further includes any of:

a time stamp of first authentication to said network service by said entity; and

a time stamp of a most recent authentication to said network service by said entity.

48. The method of Claim 47, said data object including a client identifier.

49. The method of Claim 48, said client identifier comprising any of:

a client identifier assigned by said network service; and

a client identifier provided by the client.

50. The method of Claim 45, further comprising the step of:

encrypting said trust token.

51. The method of Claim 50, further comprising a step of:

transmitting said trust token from said network service to said client upon successful authentication to said network service by said entity.

52. The method of Claim 51, wherein said the step of:

transmitting said trust token occurs via a secure channel.

53. The method of Claim 52, wherein said secure channel comprises a network connection secured via the SSL (secure sockets layer) protocol.

54. The method of Claim 49, further comprising the step of:

storing said issued trust token on said client.

55. The method of Claim 54, further comprising the step of:

transmitting said stored issued trust token along with said user ID, authentication credentials, and client identifier from said client to said network service.

56. The method of Claim 55, wherein said step of transmitting said stored, issued trust token occurs via a secured channel.

57. The method of Claim 56, wherein said secured channel comprises a network connection secured via the SSL (secure sockets layer) protocol.

58. The method of Claim 50, further comprising the step of:

storing said issued trust token in a server side database, indexed according to a combination of user ID and client identifier.

59. The method of Claim 58, further comprising the step of:

transmitting said client identifier assigned by said network service from said network service to said client upon successful authentication to said network service by said entity.

60. The method of Claim 59, wherein said step of transmitting said client identifier assigned by said network service occurs via a secure channel.

61. The method of Claim 59, said secure channel comprising a network connection secured via the SSL (secure sockets layer) protocol.

62. The method of Claim 58, further comprising the steps of:

transmitting said user ID and client identifier to said server; and

retrieving said stored trust token from said database.

63. The method of Claim 58, wherein said server side database serves a plurality of services.

64. The method of Claim 40, wherein processing requests from said trusted entities according to a first policy comprises the steps of:

validating said trust token; and

processing without adding incremental response latency.

65. The method of Claim 64, wherein said step of validating said trust token comprises the step of:

verifying that the user ID and a client identifier in the trust token match those presented by the client on the request.

66. The method of Claim 65, wherein said step of validating said trust token further comprises any of the steps of:

verifying that a time stamp of a first authentication by the entity recorded in the trust token is no earlier than a configurable earliest acceptable first-authentication time stamp; and

verifying that a time stamp of a last authentication by the entity recorded in the trust token is no earlier than a configurable earliest acceptable last-authentication time stamp.

67. The method of Claim 40, wherein processing remaining requests according to at least a second policy comprises adding a configurable amount of incremental response latency when processing untrusted logins.

68. The method of Claim 67, wherein untrusted logins include successful and unsuccessful logins.

69. The method of Claim 68, wherein response latency is added to a configurable percentage of successful logins.

70. The method of Claim 40, wherein processing remaining requests according to at least a second policy comprises adding a configurable amount of incremental response latency when processing requests from IP addresses that have exceeded a configurable login rate.

71. The method of Claim 40, wherein processing remaining requests according to at least a second policy comprises requiring an untrusted entity to complete a Turing test.

72. The method of Claim 39, wherein said policies are applied by a server.

73. The method of Claim 72, wherein said server applies rate policies for a plurality of network devices.

74. The method of Claim 44, further comprising the step of:

updating said trust token after a login by a trusted entity.

75. A method of establishing an entity requesting a network service as trusted, comprising the steps of:

for each successful authentication, adding or updating a database record containing at least a user identifier, an originating network address and a date/timestamp of first and/or the current successful authentication;

comparing all subsequent authentication requests to said record; and

where the user identifier of a subsequent request matches that of a successful authentication, extending trust to the subsequent request if its originating network address and timestamp information satisfy predetermined criteria in relation to said record.

76. The method of Claim 75, wherein said step of adding or updating a database record comprises either of the steps of:

creating a new record by said network service if an entity has not previously authenticated to said network service; and

updating a previously created record for subsequent authentication requests from said entity.

77. The method of Claim 75, wherein a network address comprises an IP (internet protocol) address.

78. The method of Claim 75, wherein the step of extending trust to the subsequent request comprises:

extending trust if the user identification and originating network address match those of the record exactly, and wherein the data/timestamps from the record satisfy configurable bounds checks.

79. The method of Claim 75, wherein the step of extending trust to the subsequent request comprises:

when the user identifier of the subsequent request matches that of a record, determining a trusted address range for the user identifier from stored authentication records.

80. The method of Claim 79, wherein the step of extending trust to the subsequent request further comprises:

if the originating address of the subsequent request falls within the trusted address range, and

determining if the data/timestamps for the trusted address range satisfy configurable bounds checks.

81. The method of Claim 79, wherein the step of determining if the data/timestamps for the trusted address range satisfy configurable bounds checks comprises the steps of:

establishing earliest date/timestamp for the trusted IP range as a minimum for the earliest authentication timestamp; and

establishing earliest date/timestamp for the trusted IP range as a maximum for the earliest authentication timestamp.

82. The method of Claim 79, wherein the step of extending trust to the subsequent request further comprises:

if the timestamps pass configurable bounds checks, extending trust to the request.

83. The method of Claim 75, wherein the entity comprises a user requesting the network service from an anonymous client.

84. The method of Claim 83, wherein the network service comprises a server.

85. The method of Claim 84, wherein the client and the server are in communication via a secured network channel.

86. The method of Claim 85, said secure channel comprising a network connection secured via the SSL (secure sockets layer) protocol

87. The method of Claim 75, further comprising the steps of:

processing requests from trusted entities according to a first policy; and

processing remaining requests according to at least a second policy.

88. The method of Claim 87, wherein processing remaining requests according to at least a second policy comprises adding a configurable amount of incremental response latency when processing untrusted logins.

89. The method of Claim 88, wherein untrusted logins include successful and unsuccessful logins from untrusted entities.

90. The method of Claim 89, wherein response latency is added to a configurable percentage of successful untrusted logins.

91. The method of Claim 87, wherein processing remaining requests according to at least a second policy comprises adding a configurable amount of incremental response latency when processing requests from IP addresses that have exceeded a configurable login rate.

92. The method of Claim 87, wherein processing remaining requests according to at least a second policy comprises requiring an untrusted entity to complete a Turing test.

93. The method of Claim 87, wherein said policies are applied by a server.

94. The method of Claim 91, wherein said server applies rate policies for a plurality of network devices.